

Vendor: Check Point

Exam Code: 156-215.71

Exam Name: Check Point Certified Security Administrator R71

Version: DEMO

QUESTION 1

You need to completely reboot the Operating System after making which of the following changes on the Security Gateway? i.e. the command cprestart is not sufficient.

A. 3 only

- B. 1, 2, 3, 4, and 5
- C. 2, 3 only
- D. 3, 4, and 5 only

Answer: C

QUESTION 2

Of the following, what parameters will not be preserved when using Database Revision Control?

Simplified mode Rule Bases
 Traditional mode Rule Bases
 Secure Platform WebUI Users
 SIC certificates
 SmartView Tracker audit logs
 SmartView Tracker traffic logs
 Implied Rules
 IPS Profiles
 Blocked connections
 Manual NAT rules
 VPN communities
 Gateway route table
 Gateway licenses

A. 3, 4, 5, 6, 9, 12, 13
B. 5, 6, 9, 12, 13
C. 1, 2, 8, 10, 11
D. 2, 4, 7, 10, 11

Answer: B

QUESTION 3

To reduce the information given to you in SmartView Tracker, what can you do to find information about data being sent between pcosaka and pctokyo?

- A. Double-click an entry representing a connection between both endpoints.
- B. Press CTRL+F in order to open the find dialog, and then search the corresponding IP addresses.
- C. Apply a source filter by adding both endpoint IP addresses with the equal option set.
- D. Use a regular expression to filter out relevant logging entries.

Answer: C

QUESTION 4

A third-shift Security Administrator configured and installed a new Security Policy early this morning. When you arrive, he tells you that he has been receiving complaints that Internet access is very slow. You suspect the Security Gateway virtual memory might be the problem. Which

SmartConsole component would you use to verify this?

- A. SmartView Tracker
- B. SmartView Monitor
- C. This information can only be viewed with fw ctl pstat command from the CLI.
- D. Eventia Analyzer

Answer: B

QUESTION 5

From the output below, where is the fingerprint generated?

Smart	Dashboard® Check Poin
R71	
This is the first ti	me you are contacting this server.
Server:	192 168 25 101 - 192 168 25 101
Eingerprint:	DEL YES HIRE KANE ATE BOOK OW NED COED FROM GO HILL
To be absolutely management, co on the server, to	y sure that no one is impersonating your ompare the Fingerprint in the Configuration Tool this Fingerprint.
	this Fingerprint as valid?
C	Approve Quat

- A. SmartUpdate
- B. Security Management Server
- C. SmartDashboard
- D. SmartConsole

Answer: B

QUESTION 6

When troubleshooting NAT entries in SmartView Tracker, which column do we need to check to view the new source IP when using NAT?

- A. XlateSrc
- B. XlateSPort
- C. XlateDst
- D. XlateDPort

Answer: A

QUESTION 7

When troubleshooting NAT entries in SmartView Tracker, which column do we need to check to view the NAT'd source port when using source NAT?

- A. XlateDst
- B. XlateDPort
- C. XlateSPort
- D. XlateSrc

Answer: C

QUESTION 8

Which Client Authentication sign-on method requires the user to first authenticate via the User Authentication mechanism when logging in to a remote server with Telnet?

- A. Standard Sign On
- B. Manual Sign On
- C. Agent Automatic Sign On
- D. Partially Automatic Sign On

Answer: D

QUESTION 9

When selecting an authentication scheme for a user, which scheme would you use if you only want the password to be stored locally?

General Properties Groups Authentication	Authentication		
Location Time	Authentication Scheme	Undefined	~
Certificates Encryption	Settings	Undefined SecurID Check Point Password OS Password RADIUS TACACS	
		No Specific Settings	

(The password is not stored at a third party component.)

- A. Check Point Password
- B. TACACS
- C. SecurID
- D. OS Password

Answer: A

QUESTION 10

Phase 2 uses ______, if not using Perfect Forward Secrecy.

- A. Symmetric
- B. Conditional
- C. Sequential
- D. Asymmetric

Answer: A

QUESTION 11

The third-shift Administrator was updating Security Management Server access settings in global properties. He managed to lock all of the administrators out of their accounts. How should you unlock these accounts?

- A. Login to SmartDashboard as the special cpconfig_admin user account, right click on administrator object and select Unlock.
- B. Type fwm lock_admin -ua from the command line of the Security Manager server.
- C. Reinstall the Security Management Server and restore using upgrade_import.
- D. Delete the file admin.lock in the \$fwDIR/tmp/ directory of the Security Management server.

Answer: B

QUESTION 12

You find a suspicious connection from a problematic host. You decide that you want to block everything from that whole network, not just the problematic host. You want to block this for an hour while you investigate further, but you do not want to add any rules to the Rule Base. How do you achieve this?

- A. Add a "temporary" rule using SmartDashboard and select hide rule.
- B. Create a Suspicious Activity Rule in SmartView Monitor
- C. Use dbedit to script the addition of a rule directly into the Rule Bases_5_0. fws configuration file.
- D. Select block intruder from the tools menu in SmartView Tracker.

Answer: B

QUESTION 13

The Check Point Security Gateway's virtual machine (kernel) exists between which two layers of the OSI model?

- A. Session and Network layers
- B. Application and Presentation layers
- C. Physical and Data link layers
- D. Network and Data link layers

Answer: D

QUESTION 14

Phase 1 uses_____

- A. Conditional
- B. Sequential
- C. Asymmetric
- D. Symmetric

Answer: C

QUESTION 15

What is a possible reason for the IKE failure shown in this screenshot?

Product Date Time Number Type Drigin	VPN-1 Power/UTM 21Jul2009 15:13:03 6503 Log fwsingapore	Action Rule Current Rule Number Rule Name User	D-= Key Install
Source Destination Service Protocol Interface Source Port	fwfrankfurt (172.30.110.1) fwsingapore (172.28.108.1) daemon 	Encryption Scheme IKE Initiator Cookie IKE Responder Cookie VPN Peer Gateway Subproduct VPN Feature	IKE 3328abc431cf19f6 2917fdf5a8c831e3 fwfrankfurt (172.30.110.1) VPN IKE IKE: Phase1 Received
Policy Name Policy Date Policy Management	-	Information	Notification from Peer: payload malformed

- A. Mismatch in VPN Domains.
- B. Mismatch in Diffie-Hellman group.
- C. Mismatch in encryption schemes.
- D. Mismatch in preshared secrets.

Answer: D

QUESTION 16

Which of the following uses the same key to decrypt as it does to encrypt?

- A. Asymmetric encryption
- B. Symmetric encryption
- C. Certificate-based encryption
- D. Dynamic encryption

Answer: A

QUESTION 17

When configuring the network interfaces of a checkpoint Gateway, the direction can be defined as Internal or external. What is meaning of interface leading to DMZ?

neral Topology	Member Network	QoS M	luiticast Restr	ictions
opology —				
External (leads	out to the Internet;)		
) Internal (leads t	o the local network	<)		
IP Addresses	behind this interfa	ice:		
Not Defin	ed			
Network	defined by the inte	face IP and I	Net Mask	
Specific:		1	*	New
✓ Interface	leads to DMZ			
unti-Spoofing	-			
Perform Anti-Sp	oofing based on in	terface topoli	127	
Don't che	ick packets from:		*	New
Spool Track	ing. 🔘 None	O 100	O Bert	

- A. It defines the DMZ Interface since this information is necessary for Content Control.
- B. Using restricted Gateways, this option automatically turns off the counting of IP Addresses originating from this interface
- C. When selecting this option. Ann-Spoofing is configured automatically to this net.
- D. Activating this option automatically turns this interface to External

Answer: A

QUESTION 18

For which service is it NOT possible to configure user authentication?

A. HTTPS

- B. FTP
- C. SSH
- D. Telnet

Answer: C

QUESTION 19

What can NOT be selected for VPN tunnel sharing?

- A. One tunnel per subnet pair
- B. One tunnel per Gateway pair
- C. One tunnel per pair of hosts
- D. One tunnel per VPN domain pair

Answer: D

QUESTION 20

You run cpconfig to reset SIC on the Security Gateway. After the SIC reset operation is complete, the policy that will be installed is the

- A. Last policy that was installed
- B. Default filter
- C. Standard policy
- D. Initial policy

Answer: D

★ Instant Download ★ PDF And VCE ★ 100% Passing Guarantee ★ 100% Money Back Guarantee

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

- ★ More than 99,900 Satisfied Customers Worldwide.
- ★ Average 99.9% Success Rate.
- ★ Free Update to match latest and real exam scenarios.
- ★ Instant Download Access! No Setup required.
- ★ Questions & Answers are downloadable in PDF format and VCE test engine format.



- ★ Multi-Platform capabilities Windows, Laptop, Mac, Android, iPhone, iPod, iPad.
- ★ 100% Guaranteed Success or 100% Money Back Guarantee.
- ★ Fast, helpful support 24x7.

View list of all certification exams: <u>http://www.braindump2go.com/all-products.html</u>



10% Discount Coupon Code: BDNT2014